USAWC STRATEGY RESEARCH PROJECT

A PARADIGM FOR THE SYSTEM OF SYSTEMS COUNTERING ASYMMETRIC ENEMY KINETIC ATTACKS

by

Colonel Karl Reinhard
United States Army

Dr. William Pierce
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 MAR 2005		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Paradigm for the System of Systems Countering Asymmetric Enemy Kinetic Attacks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Karl Reinhard	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**38**	

ABSTRACT

AUTHOR: Colonel Karl Reinhard

TITLE: A Paradigm For The System Of Systems Countering Asymmetric Enemy Kinetic Attacks

FORMAT: Strategy Research Project

DATE: 18 March 2005 PAGES: 38 CLASSIFICATION: Unclassified

Given the long history of asymmetric warfare kinetic attacks coupled with what is likely to be extended warfare against terrorism, the Army urgently needs to put effective, long-term capabilities in place to understand, evaluate, and neutralize or defeat asymmetric kinetic attacks. These measures are necessary not only to defend U.S. interests but also to provide a capability to aid our allies in their own efforts to combat asymmetric attacks.

First, the paper examines characteristics of a system of systems needed to counter asymmetric kinetic attacks that emphasizes rapidly generating and effectively employing specialized knowledge, skills, experience, and materiel to neutralize and defeat asymmetric kinetic attacks. The focus is conceptualizing the organizations and processes for rapidly arming soldiers with skills and equipment to effectively counter asymmetric kinetic attacks. These concepts are intended to complement, but not replace, other doctrine for countering insurgency and terrorism.

Second, the paper examines operational and institutional initiatives undertaken that are the first steps to establishing the required system of systems. The Army has made major strides since Operation Enduring Freedom began in late 2001. However, there is still significant work to be done to firmly establish new organizations and processes that set the stage for effectively countering asymmetric kinetic attacks.

Finally, the paper makes recommendations in six major areas to counter emerging and future asymmetric kinetic threats. These include enhancing intelligence processes, implementing a proposed skunk works-like organization focused on asymmetric kinetic threats, tightly linking this organization to newly organized technical CBRNE operational capabilities, streamlining Army institutional processes delivering solutions to asymmetric attacks, and embedding expertise in the UE_y and UE_x organizational designs.

TABLE OF CONTENTS

ABSTRACT ..... **iii**

LIST OF ILLUSTRATIONS ..... **vii**

A PARADIGM FOR THE SYSTEM OF SYSTEMS COUNTERING ASYMMETRIC ENEMY KINETIC ATTACKS **1**

LINES OF OPERATIONS FOR COUNTERING ASYMMETRIC KINETIC ATTACKS **6**

THE ARMY SYSTEM OF SYSTEMS FOR COUNTERING ASYMMETRIC KINETIC ATTACKS **8**

SYSTEM OF SYSTEMS QUALITIES **11**

ARMY OPERATIONAL INITIATIVES COUNTERING ASYMMETRIC KINETIC ATTACKS **13**

RAPID EQUIPPING FORCE **13**

IED TASK FORCE **14**

JOINT IED TASK FORCE **16**

20TH SUPPORT COMMAND (CBRNE) **17**

ARMY INSTITUTIONAL INITIATIVES COUNTERING ASYMMETRIC KINETIC ATTACKS **18**

CONCLUSIONS **20**

RECOMMENDATIONS **21**

ENDNOTES **25**

BIBLIOGRAPHY **29**

LIST OF ILLUSTRATIONS

FIGURE 1. TERRORIST INCIDENTS AND DEATHS 1980-2004 2
FIGURE 2. PIE CHART TERRORIST INCIDENTS BY TACTIC 1980-2004 2
FIGURE 3. SYSTEM OF SYSTEMS FOR COUNTERING KINETIC ATTACKS 6

A PARADIGM FOR THE SYSTEM OF SYSTEMS COUNTERING ASYMMETRIC ENEMY KINETIC ATTACKS

> In preempting the terrorist are we really dealing with asymmetry, or is something else at work? Thinking of the threat as only asymmetric misses the mark, especially if we have the concept wrong. The combination of asymmetry and the terrorists' ability to devise idiosyncratic approaches presents our real challenge.
>
> - General (Ret) Montgomery Meigs[1]

In the war on terrorism, the United States faces age-old enemies in new, more dangerous forms. With the advantages of wide-spread, modern technology, today's terrorists and insurgents are more agile and able to cause more damage both physically and psychologically than at any previous time in history. The United States faces significant challenges in developing, emplacing, and exercising the agile capabilities necessary to contain terrorist activity. Today, the challenge is most visible as U.S. armed forces working in concert with coalition partners press the fight to eliminate insurgent forces in Iraq and Afghanistan. While these are the most visible and active fronts in the war on terror, the United States and its allies battle terrorists in many other locations at home and abroad who seek to fundamentally change our way of life. At all levels of government, the United States must be prepared to face fanatically determined enemies that will change their form and methods as they relentlessly pursue our vulnerabilities.

Historically, terrorists have, more often than not, employed kinetic (or physical) attacks to achieve their ends. Over the past 25 years, there has been a dramatic increase in both the number of terrorist incidents and deaths as shown in Figure 1. Between 1968 and 2004, over 50 percent of terrorist attacks reported worldwide involved bombings and another 40 percent involved armed attack, assassination, or kidnapping – see Table 1 and associated Figure 2. Since the 1983 bombing of the Marine barracks in Lebanon, U.S. armed forces have experienced increasingly frequent asymmetric kinetic attacks including the Kohbar Towers bombing in 1996, the USS Cole attack in 2000, and numerous attacks in Afghanistan since 2001. Despite these harbingers foreshadowing the nature of modern asymmetric warfare, U.S. military forces were not fully prepared for the intensity of the insurgent attacks following its initial success in Operation Iraqi Freedom (OIF) – and in particular innovative attacks employing new tactics and improvised explosive devices (IEDs). In Iraq between 1 April 2003 and 30 November 2004, 9876 IED attacks resulted in 413 coalition force members killed in action and 4176 coalition force members wounded in action. During the same period, the insurgents exacted a heavy toll upon the Iraqi people with 1372 killed and 4396 wounded by IED attacks.[2]

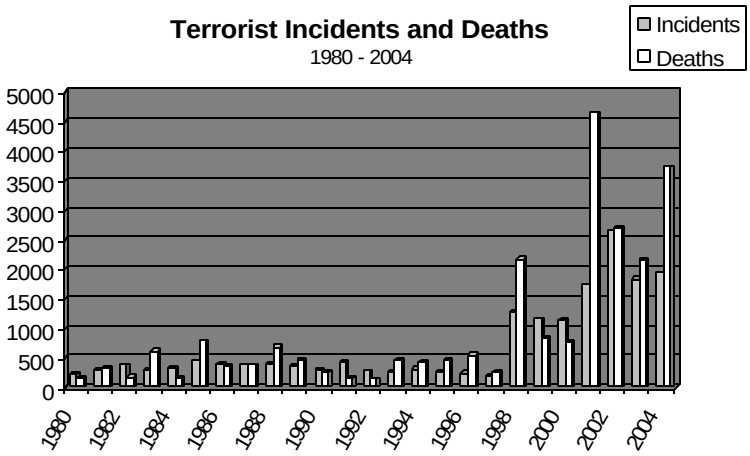


FIGURE 1 TERRORIST INCIDENTS AND DEATHS 1980-2004[3]

Tactic	Incidents	Injuries	Fatalities
Armed Attack	3726	10796	4393
Arson	533	127	268
Assassination	1882	844	2491
Barricade/Hostage	131	784	611
Bombing	9385	49231	11707
Hijacking	128	291	444
Kidnapping	1372	116	558
Other	367	644	3431
TOTAL	17524	62833	23903

TABLE 1. TERRORIST INCIDENTS BY TACTIC 1980-2004 [4]

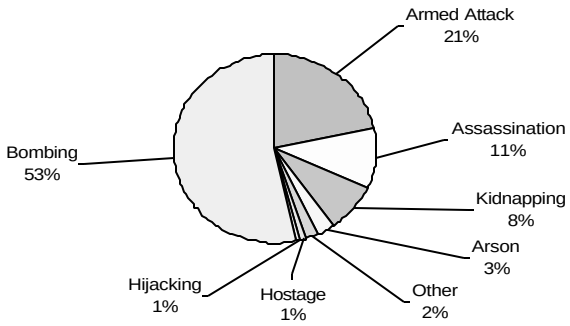


FIGURE 2. PIE CHART TERRORIST INCIDENTS BY TACTIC 1980-2004[5]

Given the long history of asymmetric warfare kinetic attacks coupled with what is likely to be extended warfare against terrorism, the Army urgently needs to put effective, long-term capabilities in place to understand, evaluate, and neutralize or defeat asymmetric kinetic attacks. These measures are necessary not only to defend U.S. interests but also to provide a capability to aid our allies in their own efforts to combat asymmetric attacks. While Department of Defense (DoD) and Army main efforts are focused on combat operations outside the United States and installation anti-terrorism force protection (ATFP) inside the United States, they both must be prepared, when directed, to support domestic civil authorities countering asymmetric kinetic attacks. This paper examines characteristics of a system of systems to counter kinetic attacks with emphasis on rapidly generating and effectively employing specialized knowledge, skills, experience, and materiel to neutralize and defeat asymmetric kinetic attacks. The focus is conceptualizing the organizations and processes for rapidly arming soldiers with skills and equipment to effectively counter asymmetric kinetic attacks; these concepts are intended to complement other doctrine for countering insurgency and terrorism. Following the 11 September 2001 terrorist attacks, the Army recognized that changes were necessary and has taken steps to effect substantive changes. Notable measures implemented to date include the organization of the Rapid Equipping Force, the Headquarters Department of the Army (HQDA) IED Task Force (IED TF), and the 20th Support Command (Chemical, Biological, Radioactive, Nuclear, and High-yield Explosive (CBRNE)); these organizations are described later. Finally, the paper recommends additional overarching capabilities that are not already in place or progress and that are essential to facilitating agile responses to emerging and future kinetic attack methods.

Asymmetric attacks can take on many forms other than kinetic including, but not limited to, computer-networks, ballistic missile, and information. However, the methods of attack addressed in this paper will be limited to kinetic attacks because the skills, equipment, and experience necessary to counter these threats are closely related; whereas, the capabilities to counter non-kinetic attacks are fundamentally different. As previously stated, kinetic attacks include explosive devices, armed attacks, and kidnapping. Attacks involving weapons of mass destruction or effect (WMD/E) that include chemical, biological, radioactive, nuclear (CBRN) agents or devices are logically included as kinetic because they frequently involve either an explosive or other mechanical dispersion method. Consequently, the skill sets countering CBRN devices are similar to those applied to bombs and armed attacks. Following this logic, dispersed bio-toxins, such as anthrax, are included. However, communicable biological agents are excluded because combating the spread of disease involves fundamentally different skill sets – skills primarily resident in the medical and public health communities.

Both terrorist and insurgent groups use asymmetric kinetic attacks to achieve their ends. While important to the strategic and operational commanders, the distinctions between the terms terrorist and insurgent are not important to the soldier being attacked on the ground. Therefore for the purposes of this paper, the term terrorist will be used but will also imply any person or group that employs asymmetric kinetic attacks to achieve their ends.[6]

The Army structures and processes emplaced for the Cold War were designed to counter the large institutional armies that U.S. forces oriented upon as likely enemies. In general, these large armies standardized tactics, techniques, and procedures (TTP). Similarly, these armies mass produced weapons and munitions specifically designed for military use. Large-scale standardization engenders organizational and production capacity inertias that in-turn constrain the rates at which change can be effected. In contrast, successful terrorists are much more likely to rapidly change TTP to maintain the effectiveness of their attacks and for self-protection. Similarly, terrorists also are more likely to adapt readily available materials to fabricate and improvise weapons that deliver success on the battlefield. In contrast to standing armies that seek standardization to improve effectiveness, terrorists keep their enemies off balance by employing non-standard, innovative, and constantly evolving weapons.

In their most virulent forms, modern terrorists are characterized by rapid innovation that leverages ubiquitous modern technology to create deadly weapons employed in uniquely destructive ways. The rates of change of both attack TTPs and weapons are facilitated and accelerated by ubiquitous international transportation and communications networks. These trends have been clearly evident in the timescales for terrorist group introduction of sophisticated IEDs over the past 30 years. Terrorists in Northern Ireland introduced progressively more sophisticated IEDs over 30 years. Various terrorist groups introduced similarly sophisticated IEDs in South Lebanon in eight years, in Chechnya in six years, in Gaza in three years, and in Iraq in 12 months.[7] Terrorists use both physical and cyber networks to rapidly share information internally and to mine useful information from external sources.

The Army's operational pace since 1990 has been intense with forces operating in Iraq, Somalia, Bosnia, Kosovo, Afghanistan, and a host of other nations around the world. U.S. force exposure to asymmetric kinetic attack has been a thread common to most of these operations. With predictions of an extended war on terrorism, there is little evidence to suggest that operational demands will diminish in the foreseeable future. Asymmetric kinetic attacks will be long-term, dangerous threats to achieving national objectives through military power. U.S. soldiers are resourceful and will do their utmost to counter and solve the problems that present themselves. However, the innovative adversary will present new tactics and weapons that the

soldier and unit on the ground are not prepared to counter at acceptable cost. These factors provide compelling arguments for instituting effective Army system of systems to counter these attacks in the near term. The system must facilitate mission success and simultaneously minimize the risk of casualties. Army leaders at every level must understand existing and emerging threats and then quickly provide solutions to units and soldiers on the ground. Given the interdependencies inherent in joint operations, the Army must draw upon, contribute to, and synchronize with similar efforts by the other Services and agencies across DoD.

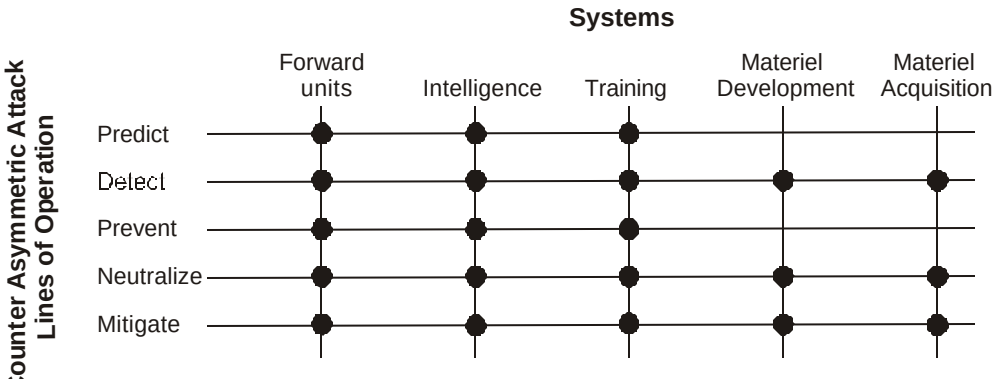
U.S. force success in asymmetric environments depends upon their ability to be more agile and adaptive than rapidly-evolving terrorist adversaries. This implies not only being prepared for known threats but also anticipating innovative threats before they emerge and being ready to effectively address unexpected threats as they emerge. Meeting the challenge demands teaming intelligence, tactical operations, training, materiel development, and materiel acquisition experts in ways that they are able to focus on adversary TTP and weapons and then deliver timely, effective solutions. Unfortunately in the post-Cold War Army, the links between these experts, when they exist, are not sufficiently responsive to counter the adversaries' ability to change TTP and weapons. Success demands dramatic advances in the Army's ability to see, understand, and act first against our adversaries' dynamic, rapidly-evolving TTP and weapons.

To meet this need for dramatic change, the Army needs inherently non-linear organizational and process approaches to replace the linear, stove-pipe, discipline-centric approaches characteristic of the Cold War Army. The Army must form an agile, solutions-oriented team (or teams) at the macro-Army level. These teams must be empowered with robust, adaptive links to the field Army and to the institutional Army having the expertise and resources to deliver solutions. As required, the teams must also have links to resources and capabilities residing in the other Services, DoD agencies, and, when appropriate, other federal or international agencies. These links should enable the two-way push and pull of information, technology, and materiel – and have the support of senior leaders. Finally, these new approaches must be recognized for the long-term requirements that they are to address long term threats.

In October 2003, the HQDA G3 established the IED Task Force to counter the IED problems encountered during OIF, which to date is the Army's center of mass for countering the IED problem at the macro-Army level. The IED TF conceptualizes the complexities of holistically countering the IED threat in two dimensions. First, the IED TF conceptualizes the on the ground actions to counter IEDs as five major activities – predict, detect, prevent, neutralize,

and mitigate.[8] For the purpose of this paper, these activities are defined as lines of operation. In the second dimension, the IED TF considered the efforts and expertise of Army "systems" that contribute to counter IED solutions. While there are many ways to define the component systems, this paper will define the following "systems" as relevant to countering asymmetric kinetic threats: forward units, intelligence, training, materiel development, and materiel acquisition.[9] A notional cross- walk of the lines of operations and the Army's supporting system of systems is shown in Figure 3.

SYSTEM OF SYSTEMS IN SUPPORT OF LINES OF OPERATION



Predict -- Activities that contribute to gathering and analyzing information about the enemy situation in order to forecast specific enemy operations directed against coalition operations

Detect -- Activities which identify locations and on-going activities to assist warfighter efforts to interdict and destroy enemy activity

Prevent -- Activities to disrupt enemy personnel; infrastructure and logistics capabilities; surveillance and targeting activities; and combat operations

Neutralize -- Activities that contribute to the destruction or reduction of enemy personnel, explosive devices, or supplies to prevent ambushes incorporating IED detonations

Mitigate -- Activities that improve survivability by reducing the threat weapon effects on its intended target

FIGURE 3. SYSTEM OF SYSTEMS FOR COUNTERING KINETIC ATTACKS[10]

LINES OF OPERATIONS FOR COUNTERING ASYMMETRIC KINETIC ATTACKS

The needs of soldiers in forward operating units to counter asymmetric kinetic attacks drive activity throughout the system of systems. Forward units are the "system" in contact with the adversary. On the ground, the lines of operation for countering kinetic attacks are interwoven with the myriad other actions the soldier routinely performs on the battlefield. In

many instances the lines of operation will be distinct and separate. However, there will also be instances when the distinctions between the lines of operation will be blurred. The following line of operation descriptions are intended to categorize activities, are not encompassing, and serve as launching points for further thought.

First, forward units need the capability to understand and template the enemy's likely attack methods and locations – the "predict" line of operation. Prediction encompasses all activities that provide insight into the adversaries' intent, capabilities, resources, and likely courses of action. Predictive analyses enable friendly forces to focus their efforts in the other lines of operation to achieve maximum effect. Intelligence and predictive analyses shape TTP development, internal force training, combat equipment, and planning for the other lines of operation. Ideally, prediction is closely integrated with center of gravity analyses, which are in turn helpful in identifying friendly and adversary critical capabilities, requirements, and vulnerabilities to focus coalition efforts.[11] During tactical operations, predictive analysis focuses soldier efforts and supporting systems on detecting actual threats at the earliest time to facilitate eliminating threats.

The "detect" line of operation encompasses the range of activities undertaken to identify the locations of enemy activity associated with asymmetric attacks. The objective is for coalition forces to detect adversary personnel, operating bases, materiel stores, and other associated infrastructure to facilitate subsequent denial and disruption. Detection may include the employment of remote sensing capabilities, physical searches, and combinations of both. Indications of adversary activity discovered may be fed to planners for deliberately planned offensive operations or be acted upon by tactical forces as targets of opportunity. During tactical operations, coalition forces are alert for indications of enemy ambushes or attacks to avoid entering kill zones.

The "prevent" line of operation starts by denying the enemy information needed to plan effective attacks – i.e. operations security. Prevent also includes deliberate offensive actions designed to deny resources and to interdict adversary operations. In some instances, friendly forces may conduct offensive search operations that combine detect and prevent activities as single integrated actions. Effective search operations require deliberate planning, search-trained soldiers, and appropriate detection equipment. Friendly forces also conduct defensive searches at entry checkpoints as force protection measures. Prevent may also include the employment of electronic and other counter-measures at stand off distances that interrupt the function of enemy weapons or disrupt his tactics. When soldiers detect potential or enemy

attacks zones, aggressive unit counter action to disrupt the attack may be considered preventing an attack.

The “neutralize” line of operation directly confronts the enemies’ offensive capabilities. Forward units may neutralize the enemy by planning and executing raids to eliminate enemy combatants, strongholds, and resources. Explosive Ordnance Disposal (EOD) soldiers may neutralize improvised explosive devices by destroying them in place or by dismantling and disposing of them. High-energy devices employed at standoff distances that destroy or otherwise neutralize the enemy or his weapons are included in this line of operation.

Finally, the “mitigate” line of operation includes protective measures taken to protect soldiers and equipment against the effects of asymmetric kinetic attacks. This includes body armor, ballistic eye protection, vehicle armor, and measures taken to harden facilities against attack. The activities described for each line of operation are representative and convey the broad array of measures that contribute to success in countering kinetic attacks. While these lines of operation are largely executed in theater, the U.S. based institutional Army with support from other Services and DoD elements have capabilities critical to rapidly and effectively countering asymmetric kinetic attacks. These supporting systems are described in the next section.

THE ARMY SYSTEM OF SYSTEMS FOR COUNTERING ASYMMETRIC KINETIC ATTACKS

Macro-Army level systems support forward-deployed units and the lines of operation countering asymmetric kinetic attack in many ways. However when dangerous new threats emerge unexpectedly, macro-Army system support may be crucial to quickly developing and introducing solutions. Today, these systems command significant resources to solve problems; however, those resources are controlled by large bureaucracies with commensurate institutional inertia. Additionally, each system is composed of multiple function-focused organizations, which may or may not act with unity of purpose under the authority of a capstone organization. Beyond providing the means to defeat asymmetric kinetic attacks, each organization also carries the burden of the multitudinous array of tasks necessary to sustain and transform an extraordinarily complex Army. The enablers supporting the lines of operation compete for attention and resources within each functional system. These systems evolved over time to meet the demands of Cold War threats and, as a consequence, are often slow to respond to today’s pressing threats.

In asymmetric warfare, the Army’s ability to win the fight depends upon its ability to identify and locate the enemy, which depends upon its intelligence system. The better its

intelligence system, the more effective the Army can be against asymmetric adversaries. The Army intelligence system reaches from forward units through intermediate units to HQDA through functional intelligence channels. The Army's intelligence system also links forward units to the broader intelligence community including DoD agencies (such as the Defense Intelligence Agency) and other federal agencies (such as the Central Intelligence Agency and the Federal Bureau of Investigation (FBI)). Optimally, timely, relevant, and accurate information flows up and down intelligence system channels to facilitate situational understanding and to shape operations. The intelligence system provides relevant information to shape actions in training and materiel development/acquisition systems. The intelligence system is the lifeblood of the "predict" line of operation and, as such, plays a critical role focusing forward unit efforts in the other lines of operation. The intelligence system systematically develops, maintains, and shares information about the cultures, actors, capabilities, and weapons within the area of operations. The intelligence system is critical to collecting, processing, and integrating information that becomes actionable intelligence that facilitates defeating the enemy. The number and persistence of asymmetric kinetic attacks in OIF demonstrates that the daunting challenges of establishing effective intelligence systems in place in the asymmetric threat environments and the gap between existing and required capabilities.

In the context of this paper, the training, materiel development, and materiel acquisition systems are most likely to provide forward units with capabilities to counter asymmetric kinetic attacks – meaning appropriately trained and equipped soldiers. The Army's Requirements Generation System provides an orderly, disciplined process for identifying required capabilities in the near, mid, and far-term. In general, the priority order for developing a capability requirement is doctrine, organization, training, leader development, personnel, facilities, and materiel (DOTMLPF).[12] The combat developer, Training and Doctrine Command (TRADOC), represents the "user" in the process. TRADOC synchronizes the efforts of the Combined Arms Center, Combined Arms Support Command, and mission area schools and centers (branches) to develop needed operational concepts, doctrine, organizations, and training requirements.[13] TRADOC and its subordinate agencies form integrated concept teams composed of stakeholders (both internal and external to the Army) to generate Army requirements, develop concepts, and record materiel operational requirements development.[14, 15] The HQDA G3 ultimately controls the prioritization of all requirements.[16]

In large measure, the Army's success depends upon the quality of its training system, which encompasses both institutional and operational training domains. Army long term success in defeating asymmetric kinetic weapons and tactics (AKW&T) will depend upon

training system decision makers understanding the existing and emerging challenges and incorporating best practice into the Army's institutional training system, resident within TRADOC and to a lesser extent in Army Materiel Command (AMC).[17] TRADOC schools and training centers conduct initial entry training and career-long professional military education for the soldiers who man forward-deployed units. Army institutional training contributes to the development of competent, confident, disciplined and adaptive leaders and soldiers. Institutional training teaches Army doctrine that is crucial to both standardization and achieving mission success.[18] TRADOC and its schools are responsible for developing doctrine, organizations, and leader development programs,[19] which form the basis for Army operations and TTP.[20] TRADOC and its schools are also responsible for developing unit structures and leader development programs. The quality of the soldiers, doctrine, and organizational designs emerging from TRADOC will strongly impact the ability of forward-deployed units to fight and decisively defeat asymmetric kinetic attacks.

The operational army builds upon institutional training through local unit training, major training events, and operational deployments. Also in the operational training domain are the combat training centers, which provide realistic and stressful training.[21] Experience gained from operational missions and combat training center exercises provide feedback for improving doctrine and TTP to TRADOC doctrine developers.[22] Ideally, the institutional and operational training domains will develop the doctrine and TTP that effectively counters adversarial TTPs before the fight. However when friendly doctrine and TTPs are not effective, lessons learned must be rapidly collected, evaluated, used to update doctrine and TTP, which in turn, are rapidly disseminated to affected units.

When materiel solutions are necessary, TRADOC combat and training developers work closely with the Army's acquisition structure to develop the materiel. The acquisition structure includes Program Executive Officers and Program/Project/ Product Managers (PMs) who report through acquisition channels to the Assistant Secretary of the Army (Acquisition, Logistics, and Technology). AMC is a key contributor to PM offices and materiel development processes through its laboratories, engineering centers, and logistics facilities.[23] Ideally, the combat developer forecasts a requirement before it is becomes critical and immediate based upon intelligence and field input. This permits the teaming of the combat and materiel developers in a measured development, acquisition, and fielding process. Then, the materiel development process is deliberate with checks and balances to ensure that the materiel fully meets the documented requirements. While this process may have proven effective during the Cold War era, it often requires painfully long development and delivery times.[24]

However when materiel solutions are urgently needed, operational field commanders may submit an operational need statement (ONS) directly to the HQDA G3, outside the combat and materiel development communities. HQDA G3 has the authority to direct a materiel solution based upon the criticality of the need, whether a materiel solution exists, and the prioritization of available resources.[25] When directed, materiel solutions should be delivered as quickly as the they can be developed, procured, and fielded. In these circumstances, a significant challenge to the materiel developers is fielding a complete solution to the soldier – including new equipment training and support packages to maintain equipment during use. The materiel fielding process must include plans to train soldiers to ensure that they are able to safely and effectively use new equipment. Compelling new equipment requirements will often dictate that new equipment training be conducted in forward areas of operation, which compounds fielding challenges. Equipment fielding must also include repair parts and maintenance procedures that can be implemented in forward operating areas.

In the context of countering kinetic attacks, urgent materiel requirements would be expected to arise from the detect, neutralize, prevent, and mitigate lines of operation. For example, materiel requirements identified during OIF for countering road-side bombs included items supporting each line of operation. Soldiers urgently needed body armor, vehicles hardened to protect against kinetic attacks, sensors to detect bombs at standoff distances, and electronic countermeasures to prevent hidden radio-controlled IEDs from detonating. EOD soldiers required both specialized EOD-specific electronic counter-measures and robotic systems to avoid unnecessary exposure to IED hazards during neutralization operations. Engineer soldiers required countermine equipment to detect and neutralize explosive ambushes and mines placed along supply routes. These examples are representative of the host of challenges faced by U.S. forces in Iraq. Compounding the challenge in Iraq was an adversary that changed tactics nearly as quickly as friendly forces developed countermeasures.

SYSTEM OF SYSTEMS QUALITIES

When engaged in high-tempo operations against a determined, innovative adversary that rapidly evolves his tactics and weapons, the Army must be as smart as, or smarter than, the enemy to defeat him. A key to success is enabling the intelligence system to develop and produce the best possible information to facilitate attacking the enemy at his weaknesses and avoiding both his strengths and attacks. When intelligence systems lack a required capability, the Army must make developing intelligence solutions a priority. Therefore, the Army's first challenge is to understand its intelligence deficiencies and purposefully develop remedies.

However when best available intelligence is inadequate and forces must engage against dangerous asymmetric adversaries, the Army must quickly develop solutions to protect soldiers. In this case, the solutions are likely to be either training- or materiel-based. The Army's challenge is to quickly understand the adversaries' tactics and weapons and then to rapidly devise solutions and methods to gain the advantage. In some instances, forward units will have the experience and skills available internally to quickly and effectively adapt intelligence processes and counter the attacks. However in many instances, forward units may not have necessary skills and experience. The overarching challenge faced today is building system of systems capabilities to develop thorough, timely intelligence information, to understand the adversaries' kinetic attacks, to develop countermeasures, and to get inside his battle rhythm to attack him – especially when the adversary adroitly employs modern technologies. While asymmetric kinetic attacks to date have largely been conventional weapons and explosives, the Army's capability to rapidly develop and integrate countermeasures must include CBRN devices and a capability to adapt to idiosyncratic kinetic attack methods that we have not considered.

To achieve the agility necessary to decisively defeat the adversary, the "solution" must:

- Be interdisciplinary and leverage seasoned experts in a variety of disciplines which include operations; intelligence; requirements development; materiel research, development and acquisition; CBRN materials and explosive devices; counterterrorism; forensic procedures, and other disciplines as appropriate.
- Have strong, credible links with the field Army to facilitate understanding the adversary and then integrating solutions into forward unit operations.
- Be able to collect, synthesize, and disseminate information and lessons learned to the field and institutional armies.
- Be able to dramatically shorten development and implementation times for training and materiel solutions.
- Be able to operate on the battlefield to complement field Army expertise and capabilities.
- Be a catalyst for developing and rapidly communicating insights to understand the enemy, to understand friendly force deficiencies, and to articulate solutions to the field and institutional Armies.
- Be a catalyst for setting in motion action that will deliver TTPs or materiel to the field Army.

An appropriate organization may well be a "skunk works," which is a small team of people who, in order to achieve unusual results, work outside the usual rules. This completes the

description of the system of systems necessary for countering asymmetric kinetic attacks. The next section describes the operationally focused organizations established since Operation Enduring Freedom (OEF) to counter asymmetric kinetic attacks.

ARMY OPERATIONAL INITIATIVES COUNTERING ASYMMETRIC KINETIC ATTACKS

> Emerging powers are studying our successes, efficiently copying our strengths and tailoring their own capabilities to attack our perceived vulnerabilities. Others are developing asymmetric strategies, developing threats that avoid or circumvent our current capabilities altogether. In the volatile, uncertain, complex and ambiguous environment we face for the foreseeable future, if we were to choose merely one advantage over our adversaries it would certainly be this: to be superior in the art of learning and adaptation. This is the imperative for a culture of innovation in the U.S. Army. [26]
>
> - Brigadier General David Fastabend
> TRADOC Futures Center

Since the U.S. began global war on terrorism operations, the Army has established several notable organizations to address requirements emerging from or related to asymmetric kinetic attacks, including the Rapid Equipping Force, the IED Task Force, and the 20th Support Command (CBRNE).

RAPID EQUIPPING FORCE

In May 2002, HQDA established the Rapid Equipping Force (REF) to provide rapid materiel solutions to support the needs of troops fighting in OEF. The REF expanded its efforts to also support OIF forces. The REF reports directly to the Vice Chief of Staff of the Army and receives operational guidance from the HQDA G3. The REF mission is three fold: first, to equip operational commanders with off-the-shelf (government or commercial) or near-term developmental items that can be quickly researched, developed, and acquired; second, to insert future force technology solutions required by engaged and deploying forces; and third, to assess capabilities and advise Army stakeholders of findings that enable forces to confront an adaptive enemy. In general, the objective is to provide equipping solutions within 90 days and developmental solutions within 360 days. The REF does not replicate the existing materiel development system and is not capable of equipping an entire theater. The REF brings solutions for in-theater evaluation and then if the solution is valuable allows units to order solutions from that point forward using the supply system.[27] Since its inception, the REF has succeeded in bringing an impressive list of solutions to forward units including biometric

devices; robots; weapons; communications equipment; and counter-IED, counter-mine, counter-sniper, counter-mortar, and force protection TTPs and materiel.[28]

IED TASK FORCE

In October 2003, HQDA established the IED TF to address Army deficiencies evident in numerous lethal asymmetric kinetic attacks in Iraq. Initially, the IED TF mission was to energize the Army's system of systems to provide solutions to the growing IED threats in Iraq and included several major efforts. To accomplish this mission, several efforts were initiated to bring together stakeholders critical to delivering short-notice solutions by pulling together experts from the HQDA staff, TRADOC, AMC, the REF, and the Army science, technology, and materiel development communities.

As a first priority, the IED TF was directed to organize and deploy small field teams of highly trained experts to Iraq. These teams were to provide liaison and assistance to forward units and to assess the in-theater challenges. Due to the short notice, the only feasible way to man the teams was to hire contractors with unique, specialized skills and experience relevant to asymmetric attacks – largely recently-retired soldiers who in the course of their careers received intense, specialized training and had gained significant operational experience. By December 2003, the IED TF had deployed two small field teams to Iraq in important first steps to developing Army solutions.

In late 2003, there were two other notable initiatives aimed at defeating IEDs. First, the DoD Combating Terrorism Technology Support Office proposed establishing an interagency organization to share technical terrorist bomb technical information among federal agencies involved in the war on terror. In December 2003, the Terrorist Explosives Device Analytical Center (TEDAC) was organized under FBI leadership with DoD and IED TF participation.[29] In this same timeframe and as a parallel action, the IED TF also took on sponsorship of the ad hoc Combined Explosives Exploitation Cell (CEXC) that had been established in the CJTF-7 headquarters to provide a center for collecting information about IEDs in Iraq. This interagency collaboration resulted as connections between bombings occurring in Afghanistan, Iraq and other disparate parts of the world became apparent. The CECX joint manning document called for 14 people including experts from the FBI, Bureau of Alcohol Tobacco and Firearms (ATF), Service EOD forces, and other federal intelligence agencies, and international partners. Interagency participation facilitates the cross fertilization of expertise between agencies and the flow of information between agencies. CEXC personnel visit bomb sites to collect information and forensic material. The CEXC performs initial exploitation of recovered information and

material, which supports in-theater terrorism counter-action.[30] The creation of these organizations represented significant steps to building interagency efforts in the war on terrorism. The TEDAC, CEXC, and IED Task Force field teams are examples of efforts to collect and share information regarding both IEDs and broader asymmetric kinetic attacks.

A year later in December 2004, the IED TF had reached maturity and was producing tangible results through four distinct elements – forward deployed field teams, the Tactical Advisory Team, the Evaluation and Integration Team, and HQDA working groups that it sponsors. The IED TF deployed teams to Afghanistan and additional field teams to Iraq. With time, the field teams have matured into several roles. In addition to their initial role of establishing liaison between the IED TF and forward units, the teams have proven themselves to be a valuable means of putting experienced operators into the field to gather information about friendly force experiences and enemy TTP and weapons. Based upon their experience, the teams perform quick assessments of new enemy TTP and weapons. The teams report their observations and assessments to both the supported unit and to other IED TF elements – expediting the flow of information to stakeholders that can provide solutions.[31] Finally, the teams provide a specialized, highly qualified resource for training friendly force trainers.

The IED TF also established the Tactical Advisory Team, which is composed of a cell embedded in the Center for Army Lessons Learned (CALL) at Fort Leavenworth and IED awareness mobile training teams. On a continuing basis, CALL collects and analyzes reports from field teams and other sources to distill lessons learned. CALL uses these lessons to develop training materials for Army-wide use, which are available to stakeholders through CALL websites. The IED awareness training teams provide on-site multi-echelon training to units preparing to deploy. The training is tailored to the needs of senior corps and division leaders, brigade and battalion leaders, and company-level leaders. The IED awareness training teams also assist the Army's Combat Training Center efforts by providing information and expertise to facilitate scenario development and evaluation.[32]

The Evaluation and Integration Team, based in the Washington DC area, integrates technology and operations – providing a link between operators and technology developers. The team reviews reports from IED TF field teams and forward deployed units to identify problems and glean possible solutions. It engages with industry partners and science and technology organizations, both Army and DoD-wide, to identify available and suitable technologies to solve pressing problems. The team makes recommendations to the IED TF, the REF, and materiel developers on promising solutions that should be vigorously pursued.[33]

Operating from the HQDA G3's Army Operation Center (AOC), the IED TF headquarters staff is the fourth distinct task force element. The IED TF staff synchronizes the efforts of the other IED TF elements, the Army staff, and other stakeholders across DoD and the federal government. The IED TF staff develops the common operating picture of the asymmetric attacks that facilitates the formulation and approval of the Army's rapidly evolving efforts to address the AKW&T challenges. The staff coordinates the efforts of several specialized working groups drawn from the HQDA and Major Command (MACOM) staffs to facilitate and synchronize the myriad of actions necessary to quickly put effective solutions on the ground. The IED TF headquarters staff has many "skunkworks" characteristics – a relatively small group of very capable people working outside of normal processes to achieve unusual results.

The IED TF was established as a temporary, ad hoc organization to address the urgent IED threat in Iraq. In recognition of projected long-term Global War on Terrorism (GWOT) operations, the HQDA G3 subsequently directed that the IED TF lead an effort to establish a permanent operationally focused organization to replace itself. The outgrowth of that directive is currently called the Asymmetric Warfare Group (AWG). In the final stages of organizational design, the AWG is projected to have a January 2005 initial operating capability. The AWG structure is expected to mirror the existing IED TF structure with robust operations and intelligence staffs, a Training Advisory Group, and a Concepts Integration Office – performing functions similar to IED TF elements previously described. The AWG is projected to have a subordinate Operations Squadron composed of four troops, with each of these having three field teams. Current planning is for the IED TF to gradually transfer responsibilities to the AWG over the course of a year. In the near term, the AWG is expected to report to the HQDA G3; although, the Army staff is debating who the AWG should report to in the long term.[34]

JOINT IED TASK FORCE

In July 2004 and in the wake of continued violence in Iraq, the Deputy Secretary of Defense (DEPSECDEF) established a Joint Integrated Process Team for Defeating Improvised Explosive Devices (Joint IED Defeat IPT) for the purpose of sharpening DoD focus on IEDs. The Joint IED Defeat IPT's purpose is to coordinate multiple efforts across DoD and other government agencies to identify near-term solutions. The Army is the designated lead for the IPT.[35] The Joint IED Defeat IPT, chaired by the Army major general directing the AOC, reports through the Vice Chief of Staff of the Army and Secretary of the Army to the DEPSECDEF. Each Service provides flag officer representation to the IPT. The Joint IPT has five subordinate IPTs built around the five functional lines of operation – predict, detect, prevent, neutralize, and

mitigate. As part of this initiative, the Army's good idea embodied in the IED TF expanded to become the Joint IED TF with each service providing manning to support task force operations.[36]

20TH SUPPORT COMMAND (CBRNE)

On 16 October 2004, United States Army Forces Command activated the 20th Support Comand (SUPCOM) (CBRNE), realigning the 22nd Chemical Battalion (Technical Escort) and the 52nd Ordnance Group (Explosive Ordnance Disposal (EOD)) as subordinate organizations to the command. The 20th SUPCOM (CBRNE) is envisioned to provide global, full-spectrum CBRNE technical response forces and capabilities to Joint and Army Force Commanders. The Department of the Army approved mission statement for the 20th SUPCOM (CBRNE) is:

> The CBRNE Command integrates, coordinates, deploys and provides trained and ready forces, and is prepared to exercise command and control of full spectrum CBRNE operations to Joint and Army Force Commanders. Maintains technical links with appropriate Joint, Federal, and State CBRNE assets, as well as research, development and technical communities to assure Army CBRNE response readiness. Provides or assists in the training and readiness oversight of CBRNE assets (Active, Guard and Reserve).[37]

The command was conceived and established in the post 11 September 2001 environment to consolidate, to the extent feasible, Army CBRNE technical operations response capabilities in a single operational command. For those capabilities not assigned, the command is the focal point for integrating Army CBRNE technical response efforts. The command's assigned forces include the 22d Chemical Battalion (formerly the Army's Technical Escort Unit, which reported through the Research, Development, and Engineering Command to the Army Materiel Command) and the 52d Ordnance Group (EOD), which are the Army's principle active duty CBRNE technical response units. Army organizations with CBRNE technical response capabilities but not assigned to the 20th SUPCOM (CBRNE) are included in the list of force pool units to be drawn upon as required. 20th SUPCOM (CBRNE) also reaches to other DoD and federal organizations for CBRNE technical response capabilities via memoranda of agreement. As the 20th SUPCOM (CBRNE) matures, it is expected to be involved in training and readiness oversight of active, guard, and reserve CBRNE technical response assets.

The 20th SUPCOM (CBRNE) performs its mission across the spectrum of operations. In peacetime domestic operations, EOD and TEU response teams provide routine response to eliminate the hazards of devices that may contain military chemical, biological, radioactive materials; improvised explosive devices ; and unexploded ordnance. 20th SUPCOM (CBRNE)

provides forces to support the U.S. Secret Service (USSS) protection of the President and other very-important persons. 20th SUPCOM (CBRNE) also provides forces to support the USSS in its role as the lead federal agency for securing National Special Security Events. In peace operations outside the U.S., 20th SUPCOM (CBRNE) conducts CBRNE technical operations supporting combatant commander regional engagement requirements. The 20th SUPCOM (CBRNE) also provides CBRNE technical advisory teams and technical response forces to support combatant commander requirements spanning the spectrum of operations up to and including small-scale contingencies and major combat operations. CBRNE technical advisory teams and response forces provide combatant commanders with the capability to search for, identify, disable, render safe, transport, and dispose of CBRNE materials. These forces provide capabilities that were not available to the ad hoc organizations created to search for weapons of mass destruction in Operation Iraqi Freedom.[38]

Task Force IED and the 20th SUPCOM are significant additional operational capabilities for countering asymmetric kinetic attacks. The next section describes institutional Army efforts to implement change to enhance its efforts to counter asymmetric kinetic attacks.

ARMY INSTITUTIONAL INITIATIVES COUNTERING ASYMMETRIC KINETIC ATTACKS

> Ultimately, our ability to rapidly adapt processes and resulting Doctrine, Organizations, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF) solutions will be the measure of the Army's agility – and proof of its culture of innovation.
>
> - Army Transformation Roadmap[39]

Concurrent with fighting in Iraq and Afghanistan, the Army is fundamentally transforming to create easily tailorable, modular forces to deliver the right force at the right time and place.[40] Change must be viewed comprehensively across the DOTMLPF imperatives, because modern land warfare is extraordinarily complex. Comprehensive DOTMLPF review seeks to avoid unintended detrimental second and third order affects. The Army and TRADOC manage change by imposing orderly processes that effect change. Many institutional processes are emplaced to establish control rather than to facilitate rapid innovation. Further complicating TRADOC's transformation is the natural resistance of successful organizations to reinvent themselves.[41] The challenge emerging with the simultaneous global war on terror and Army transformation efforts is the need to accommodate immediate requirements to change while retaining sufficient process to ensure appropriate, high-quality solutions that minimize unintended consequences. Clearly as the Army transforms, TRADOC must also adapt to

facilitate innovation in the processes and organizations that it owns to effect timely change across the DOTMLPF imperatives.

Within TRADOC, there are multiple branches and schools likely to contribute significantly to the system of systems including, but not limited to: Infantry, Engineer, Ordnance (for EOD), Military Intelligence, Chemical, Special Forces, and Transportation. A significant TRADOC challenge is assigning responsibility to lead and coordinate the efforts of diverse stakeholders from across the Army. Each branch school brings unique skill sets, perspectives, and agendas to the table. The differences are double edged swords – sometimes enhancing solutions and sometimes obstructing effective solutions. In some instances, new skill sets must be developed that are not resident in any branch or school. For instance in October 2004, the Army published Field Manual-Interim 3-07.22, *Counterinsurgency Operations* – a year after the IED TF was established. Incredibly, while the FM mentions IEDs as a peripheral threat, it does not mention operational level IED campaigns employed by an adversary, much less establish any doctrine for countering such campaigns.[42] As a second example, no branch has the skill sets appropriate for developing doctrine, TTP, or materiel for countering wireless remotely controlled IEDs.

Per Army Regulation 5-22, *The Army Proponent System* , the Combined Arms Center (CAC) has proponency for low-intensity conflict and terrorism counter action.[43] Since the formation of the IED TF, TRADOC has looked to the Maneuver Support Center (MANSCEN), a subordinate of CAC, for leading its efforts to address counter IED issues. Within MANSCEN, the Counter Explosives Hazards Center (CEHC) was created in 2003 from the Countermine Counter-Boobytrap Center to address explosive hazards. TRADOC is in the process of charting its road ahead for tackling the system of system challenges posed by IEDs. In mid-November 2004, MANSCEN hosted a general officer conference to chart the course ahead with HQDA and TRADOC participation. The resulting MANSCEN recommendation was that TRADOC charter an MANSCEN-led Integrated Concept Team (ICT) to develop recommendations for assigning proponency.[44] An ICT brings together stakeholder experts with authority to make decisions for the organization they represent. ICTs are formed for limited times to analyze the problem and to develop recommendations for long term solutions to problems.

A legacy of Cold War Army unit organizational designs is the absence of specialized technical expertise embedded in Corps and below staffs for countering asymmetric kinetic attacks. The Army's functional expertise for understanding and reacting to IEDs was in its EOD forces. However, no Army conventional warfighting headquarters had EOD staff assigned. The field Army depended upon EOD units that would be provided upon deployment for unexploded

ordnance (UXO) and IED expertise. While UXO and IEDs were sometimes played during major staff exercises or at the combat training centers, the exercise play had little, if any, impact upon the exercise. Consequently, UXO and IEDs received little, if any, attention from senior leaders or staff. During OIF, the importance of this expertise became apparent. In recognition of the lack of the importance that UXO and IEDs are likely to play in future operations, EOD staffs have been proposed additions to the UEy, UEx, and Maneuver Enhancement Brigade organizational designs in the modular Army. However to date, the addition of these positions to to new organizational designs has not been approved.

During OIF, CJTF-7 recognized the need to systematically collect technical information and organized the Counter Explosives Exploitation Cell, for which the IED TF subsequently assumed a sponsoring role. The CEXC makes important contributions to the intelligence system that is vital to developing the actionable intelligence essential to effectively attacking and defeating the asymmetric adversary. Unfortunately, the CEXC concept has not been institutionalized in doctrine or organizational designs.

CONCLUSIONS

In the space of slightly over three years, the Army has made significant progress in understanding and moving to defeat asymmetric kinetic attacks – including IEDs and CBRNE devices. Following 9/11, the Army recognized the importance of CBRNE technical response and formed the 20th SUPCOM (CBRNE). During OEF, the Army established the REF to rapidly develop and introduce prototype materiel solutions to soldiers on the ground. Within months of a broad based insurgency emerging in Iraq that forces on the ground were not well prepared to counter, HQDA reacted with purpose by establishing the IED TF as a skunk works-like organization to investigate the nature of the asymmetric threats in Iraq and to develop and implement immediate solutions outside normal Army processes. The DoD and Joint Staffs recognized the merits of the IED Task Force efforts and expanded that effort into the Joint IED Defeat Task Force – in clear recognition that asymmetric kinetic attacks threaten all Service forces. The Terrorist Explosive Device Analysis Center in the U.S. and the Counter Explosive Exploitation Cells in Iraq and Afghanistan are significant steps in collecting and exploiting technical information relevant to asymmetric kinetic attacks across DoD, the federal government, and with coalition partners.

In a little over one year, the IED TF has developed a comprehensive framework for conceptualizing the holistic asymmetric kinetic attack problem. Further, the IED Task Force has been the forcing function driving substantive changes to the Army system of systems that act to

counter asymmetric kinetic attacks – and has caused solutions to be delivered to soldiers on the ground in record time. IED Task Force success is attributable to several things. First, the IED Task Force was a single, agile, adaptive organization empowered to operate on the ground, at the HQDA staff level, with TRADOC and AMC organizations, other relevant Service elements and DoD organizations, other federal agencies, international partners and other organizations as necessary. IED Task Force efforts have produced measurable TTP, training, and materiel solution enhancements to soldiers operating on the ground. Second, the IED Task Force had the full support and backing of senior Army leaders. Significantly, HQDA has recognized the need for long-term organizations to perform the functions of the IED Task Force and is working to establish the AWG as its permanent successor.

While the Army has made major strides, there is still significant work to be done to firmly establish new organizations and processes that set the stage for effectively countering asymmetric kinetic attacks. The intensity of asymmetric kinetic attacks in Iraq show that the current intelligence system is falling short in providing the full measure of information necessary to defeat the insurgency in Iraq. While the IED TF has matured, it is only a short term bridge to a long term organizational solution; the AWG, which is envisioned to assume the lion's share of the IED TF workload. The Army has recognized the need to adapt the Army's doctrine, training, and materiel development systems – yet the process of establishing the needed organizations and streamlining DOTMLPF processes in the institutional Army has barely begun more than a year after the IED TF was established – despite TRADOC and MANSCEN being involved since the inception of the IED TF.

RECOMMENDATIONS

As it moves forward to counter emerging and future asymmetric kinetic threats, there are six major areas that the Army must attend to:

- Enhancing the intelligence system and its processes to provide the information necessary to decisively defeat terrorists in asymmetric warfare environments. This includes fully resourcing and leveraging the TEDAC and CEXC as key contributors to understanding asymmetric threats and shaping operations.
- Transitioning from the IED Task Force to a permanent operationally focused organization.
- Establishing effective, adaptive, and agile institutional Army structures and processes for training and combat developments.
- Establishing effective institutional structures for materiel development and fielding.

- Linking IED defeat efforts to 20th SUPCOM (CBRNE) operations.
- Embedding IED defeat technical operations expertise into UEy and UEx organizational designs.
- Embedding the Combined Explosives Exploitation Cell concept in doctrine and organizational designs.

The Army must carry forward the momentum gained by the IED TF in effecting organizational and process change to enable the Army to react to existing, emerging, and future asymmetric kinetic threats. It is essential that the follow-on organizations (i.e. Asymmetric Warfare Group, HQDA staff, Rapid Equipping Force, etc.) and retain the IED TF qualities that were key to success – a skunk-works like organization empowered to touch every contributing Army system with authority – and the senior leader backing to effect expeditious action. These organizations must have a strong tie to the HQDA staff to rapidly bring issues to the attention of key leaders and to accelerate resourcing and fielding processes. The AWG must build a bench of talented, highly-trained, and experienced staff to vigorously execute its mission. Finally, the follow-on organizations must work with inter-Service, joint, interagency, and international organizations to develop synergistic solutions.

The Army must quickly establish an effective structure within TRADOC to facilitate training and combat developments related to asymmetric kinetic attack defeat. Proponency for IED defeat should be assigned to the Combined Arms Center (CAC) – not to MANSCEN. CAC has the necessary oversight of MANSCEN and most of the other branch schools with a stake in the process. CAC is best positioned to integrate the diverse skill sets that contribute to defeating IEDs. CAC is also best positioned to adjudicate the competing branch and school interests – and avoid dysfunctional branch parochialisms that often paralyze sound decision-making processes within TRADOC and the Army. If necessary, CAC should assume responsibility from MANSCEN for the direction of the Counter Explosives Hazard Center to accomplish this mission. The Army and TRADOC must streamline training, combat development, and materiel development "process" to the fullest extent possible to accelerate action.

The Army must link the efforts of the 20th SUPCOM (CBRNE) and Asymmetric Warfare Group. Both organizations have technical operational missions related to CBRNE technical response. Failing to strongly link these organizations creates a seam in Army operations that may either be deliberately exploited or inadvertently limit the Army's ability to respond to CBRNE events. Since the Services are becoming increasingly interdependent, the seam would also extend to joint operations. Most asymmetric kinetic attacks have been associated with explosives, which is the common thread between these organizations. Consequently, both

organizations will have similar intelligence and technical expertise requirements. Further, the skill sets in each organization are complementary – active cross fertilization of ideas and TTP will have synergistic effects benefiting the Army. The two organizations could report to the same command. Alternatively, the AWG could report to the 20th SUPCOM (CBRNE). Finally, the two commands could reside in different MACOMs provided that direct and robust liaison is authorized on a continuing basis.

Finally in recognition that asymmetric kinetic attacks will be an enduring feature of 21st century warfare, the Army must build the capability into its new modular structure to address the challenges of countering asymmetric warfare. A lesson learned in OIF is that not having the expertise resident can be very costly. As a minimum, the UEy and UEx structures must have staff elements that understand and can facilitate the lines of operation for countering asymmetric kinetic weapons in theater. In recognition of the reality that asymmetric kinetic warfare will be significant component of future operating environments, these positions must be filled with best-qualified soldiers to provide essential expertise for planning and executing Army operations. The staff element should become a focal point for working solutions with and through the Army's system of systems to enable soldiers on the ground to fight and win against asymmetric kinetic adversaries. Finally, the Combined Explosives Exploitation Cell must be incorporated into both doctrine and organizational designs – with the connections necessary to rapidly and effectively integrate appropriate interagency representatives into operations.

WORD COUNT= 8736

ENDNOTES

[1] Montgomery C. Meigs, *Parameters* vol. 33, no. 2 (Summer 2003): 4.

[2] George Byford <ByfordG@iraq.centcom.smil.mil>m "RE: CEXC Brief," electronic mail message sent to Karl Reinhard <karl.reinhard@us.army.smil.mil>, 24 December 2004.

[3] National Memorial Institute for the Prevention of Terrorism (MIPT) Database; Internet; <http://www.tkb.org>, accessed on 14 January 2005. The MIPT database is funded by the Department of Homeland Security. The Rand Corporation verifies terrorism incidents entered in the database. Note that the database does not accurately report terrorist attacks against military targets based upon the number of CEXC reported terrorist attacks in Iraq in 2003 and 2004.

[4] Ibid.

[5] Ibid.

[6] DoD defines an insurgency as an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict. DoD defines terrorism as the calculated use of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally, political, religious, or ideological. Joint Electronic Library. <http://www.dtic.mil/doctrine/jel/doddict/index.html>; accessed 26 November 2004.

[7] Roger Davies, Hazard Management Solutions, telephone interview by author 7 January 2005. Hazard Management Solutions performs contract work for the DoD Technical Support Working Group in analyzing IED challenges and solutions. Roger Davies is retired from the British Army and commanded EOD units in Northern Ireland.

[8] The five activity areas (predict, detect, prevent, neutralize, and mitigate) were borrowed from the Army Engineer School's Assured Mobility fundamentals; however, Task Force IED is not using the "avoid" fundamental as part of its model. Task Force IED activity definitions are substantially different than the corresponding Assured Mobility activity definitions. Each TF IED activity areas encompass efforts across the full spectrum of the Army's capabilities. Consequently, the Army's counter IED activities should not be viewed as an extension of the Engineer's Assured Mobility concept.

[9] The author identified these Army systems as key to understanding the challenges associated with the counter IED problem. Task Force IED thinks in terms of a system of systems but never formally defined what it considers to be the "system of systems."

[10] Robert Hart, Strategic Communications Officer, Joint IED Defeat Task Force, interview by author, 29 Oct 04, Pentagon, Washington DC. Activity definitions were taken from the Joint IED Defeat Task Force briefing provided during the interview. The system of systems categorizations are the author's.

[11] Joe Strange, *Centers of Gravity and Critical Vulnerabilities*, (Quantico, Virginia: Marine Corps University Foundation, 1996), 43. Dr Strange's monograph links center of gravity

analysis to a hierarchy critical capabilities, requirements, and vulnerabilities. This type analysis is helpful in focusing terrorism counteraction.

[12] Department of the Army, *Materiel Requirements*, Army Regulation 71-9, (Washington, D.C.: U.S. Department of the Army, 30 April 1997), 1.

[13] Ibid, 5.

[14] Ibid, 1.

[15] Department of the Army, *Requirements Determination*, Training and Doctrine Command Pamphlet 71-9 (Fort Monroe, VA: Headquarters, Training and Doctrine Command, 5 November 1999), 13.

[16] Army Regulation 71-9, 2.

[17] Department of the Army, *Battle Focused Training*, Field Manual 7-1 (Washington, D.C.: U.S. Department of the Army, 15 September 2003), 1-9. AMC conducts specialized materiel readiness training; is the HQDA G3 executive agent for new equipment (NET) training; assists in the development and acquisition of specialized training products.

[18] Department of the Army, *Training the Force*, Field Manual 7-0 (Washington, D.C.: U.S. Department of the Army, 22 October 2002), 1-7 to 1-8.

[19] Department of the Army, *The Army Proponent System* , Army Regulation 5-22 (Washington, DC: U.S. Department of the Army, 3 October 1986), 1.

[20] Department of the Army, *The TRADOC Doctrinal Literature Program* , TRADOC Regulation 25-36 (Headquarters TRADOC, Fort Monroe, VA, 1 October 2004), 17-19.

[21] Training the Force, 1-11.

[22] Ibid, 1-11.

[23] Army Regulation 71-9, 4-7.

[24]Tim Kennedy, "TRADOC Seeks Wartime Solutions From Rapid Equipping Force," *Army*, vol. 54, no. 8 (August 2004): 42. BG Phillip Coker, Director Capabilities Development Center, TRADOC Futures Center is quoted, "For TRADOC, it often takes three to five years to get a capability into the hands of a soldier, even when we're working very hard at all the right things as quickly as possible."

[25] Ibid, 1.

[26] David A. Fastabend and Robert H. Simpson, "The Imperative for a Culture of Innovation in the U.S. Army: Adapt or Die," *Army Magazine*, February 2004; available from <http://www.ausa.org/www/armymag.nsf/0/EB5252A9404F977685256E220059F541?OpenDoc

ument>; Internet; accessed on 11 December 2004. Brigadier General Fastabend was serving as the Director, Concept Development and Experimentation, Futures Center, TRADOC.

[27] Department of the Army, "Rapid Equipping Force" available from <https://www.ref.army.mil/textonly/default.html>; Internet; accessed 4 December 2004.

[28] Paul Stoskus, Deputy Director Rapid Equipping Force, "Rapid Equipping Force Briefing to International Armaments and Technology Exhibition, 16 June 2004," available from <http://www.dtic.mil/ndia/2004armaments/DayII/SessionII/06Stoskus_Rapid_Equipment_Force.pdf>; Internet; accessed 4 December 2004.

[29] David Johnston, "U.S. Agency Sees Global Network for Bomb Making," *New York Times*, 22 February 2004, late edition-final, sec 1, p. 1, col 6.

[30] George Byford <ByfordG@iraq.centcom.smil.mil> "CEXC Brief," electronic mail message sent to Karl Reinhard <karl.reinhard@us.army.smil.mil>, 17 December 2004.

[31] Hart in author interview 29 Oct 04. From briefing materials provided.

[32] Ibid.

[33] Ibid.

[34] Michael Bowman, Staff Officer, Joint IED Defeat Task Force, interview by author, 29 Oct 04, Pentagon, Washington DC. He provided "Asymmetric Warfare Group Update" briefing dated 7 October 2004 for reference.

[35] Deputy Secretary of Defense Paul Wolfowitz, "Joint Integrated Process Team (IPT) for Defeating Improvised Explosive Devices," memorandum for Secretaries of the Military Departments, Washington, D.C., 17 July 2004.

[36] Hart in author interview 29 Oct 04. From "Joint IED Task Force Briefing" slides provided.

[37] Headquarters Department of the Army, Operational and Organizational (O&O) Concept for the Chemical, Biological, Radiological, Nuclear, and High Yield Explosives (CBRNE) Operations Headquarters (version 6.8) (Headquarters Training and Doctrine Command, Force Design Division, Fort Leavenworth, KS, February 2004), 20. Memorandum submitted through HQ TRADOC to HQDA G3. Concept was approved for implementation by HQDA; 20th Support Command (CBRNE) was established on 16 October 2004.

[38] Ibid. 21-25.

[39] Department of the Army, *United States Army Transformation Roadmap* (Washington, D.C.: U.S. Department of the Army, 1 November 2003), x.

[40] Ibid. 1-11.

[41] Fastabend.

[42] Department of the Army, *Counterinsurgency Operations*, Field Manual-Interim 3-07.22 (Washington, D.C.: U.S. Department of the Army, 1 October 2004). In the Field Manual, IEDs are discussed at the standard operating procedure level – no mention made of the system of systems necessary to counter an operational level IED campaign.

[43] Army Regulation 5-22, *The Army Proponency System*, 2.

[44] Commander, Maneuver Support Center, "Action Plan – Counters to Improvised Explosive Devices (IED)," memorandum for Deputy Commander / Chief of Staff, Headquarters Training and Doctrine Command, Fort Leonard Wood, Missouri, 23 November 2004.

BIBLIOGRAPHY

Bowman, Michael, Staff Officer, Joint IED Defeat Task Force. Interview by author. 29 October 2004, Pentagon, Washington DC.

Byford, George <ByfordG@iraq.centcom.smil.mil>. "CEXC Brief." Electronic mail message sent to Karl Reinhard <karl.reinhard@us.army.smil.mil>. 17 December 2004.

_____. "RE: CEXC Brief," Electronic mail message sent to Karl Reinhard <karl.reinhard@us.army.smil.mil>. 24 December 2004.

Commander, U.S. Army Maneuver Support Center, "Action Plan – Counters to Improvised Explosive Devices (IED)." Memorandum for Deputy Commander / Chief of Staff, Headquarters, Training and Doctrine Command. Fort Leonard Wood, Missouri, 23 November 2004.

Davies, Roger, Hazard Management Solutions. Telephone interview by author, 7 January 2005.

Fastabend, David A. and Robert H. Simpson. "The Imperative for a Culture of Innovation in the U.S. Army: Adapt or Die." *Army Magazine*, February 2004. Available from <http://www.ausa.org/www/armymag.nsf/0/EB5252A9404F977685256E220059F541?OpenDocument>. Internet. Accessed 11 December 2004.

Hart, Robert, Strategic Communications Officer, Joint IED Defeat Task Force. Interview by author, 29 October 2004, Pentagon, Washington DC.

Johnston, David. "U.S. Agency Sees Global Network for Bomb Making." *New York Times*, 22 February 2004, late edition-final, sec. 1, p. 1, col. 6.

Joint Electronic Library. Available from <http://www.dtic.mil/doctrine/jel/doddict/index.html>. Accessed 26 November 2004.

Kennedy, Tim. "TRADOC Seeks Wartime Solutions From Rapid Equipping Force," *Army*, vol 54, no. 8 (August 2004): 39 – 42.

Meigs, Montgomery C. "Unorthodox Thoughts About Asymmetric Warfare." *Parameters* vol 33, no. 2 (Summer 2004): 4 – 18.

National Memorial Institute for the Prevention of Terrorism (MIPT) Database. Available from <http://www.tkb.org>. Internet. Accessed 14 January 2005.

Stoskus, Paul, Deputy Director Rapid Equipping Force. "Rapid Equipping Force Briefing to International Armaments and Technology Exhibition, 16 June 2004." Available from <http://www.dtic.mil/ndia/2004armaments/DayII/SessionII/06Stoskus_Rapid_Equipment_Force.pdf>. Internet. Accessed 4 December 2004.

Strange, Joe. *Centers of Gravity and Critical Vulnerabilities*. Quantico, Virginia: Marine Corps University Foundation, 1996.

U.S. Department of the Army, "Rapid Equipping Force." Available from <https://www.ref.army.mil/textonly/default.html>. Internet. Accessed 4 December 2004.

U.S. Department of the Army. "Operational and Organizational (O&O) Concept for the Chemical, Biological, Radiological, Nuclear, and High Yield Explosives (CBRNE) Operations Headquarters (version 6.8)." Fort Leavenworth, KS: Training and Doctrine Command, Force Design Directorate, February 2004.

U.S. Department of the Army. *Battle Focused Training*. Field Manual 7-1. Washington, D.C.: U.S. Department of the Army, 15 September 2003.

U.S. Department of the Army. *Counterinsurgency Operations*. Field Manual-Interim 3-07.22. Washington, D.C.: U.S. Department of the Army, 1 October 2004.

U.S. Department of the Army. *Materiel Requirements*, Army Regulation 71-9. Washington, D.C.: U.S. Department of the Army, 30 April 1997.

U.S. Department of the Army. *Requirements Determination*, Training and Doctrine Command Pamphlet 71-9. Fort Monroe, VA: Headquarters, Training and Doctrine Command, 5 November 1999.

U.S. Department of the Army. *The Army Proponent System* . Army Regulation 5-22. Washington, D.C.: Department of the Army, 3 October 1986.

U.S. Department of the Army. *The TRADOC Doctrinal Literature Program* , Training and Doctrine Command Regulation 25-36. Fort Monroe, VA: Headquarters, Training and Doctrine Command, 1 October 2004.

U.S. Department of the Army. *Training the Force*. Field Manual 7-0. Washington, D.C.: U.S. Department of the Army, 22 October 2002.

U.S. Department of the Army. *United States Army Transformation Roadmap.* Washington, D.C.: U.S. Department of the Army, 1 November 2003.

Wolfowitz, Paul, Deputy Secretary of Defense. "Joint Integrated Process Team (IPT) for Defeating Improvised Explosive Devices." Memorandum for Secretaries of the Military Departments. Washington, D.C., 17 July 2004.